SIGMA
JURNAL TEKNOLOGI PELITA BANGSA

Vol.14 No.3 September 2023 p-ISSN: 2407-3903 e-ISSN: 2407-3903

Diterima, 21 Agustus 2023 | Direvisi, 26 Agustus 2023 | Dipublikasikan, 6 September 2023

IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) BERBASIS WEB (STUDI KASUS : PT BANK TABUNGAN NEGARA)

Ahmad Turmudi Zy[1], Isarianto[2], Arif Susilo[3], Alif Mustafanah[4]

[1]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]turmudi@pelitabangsa.ac.id, [2]irianto@pelitabangsa.ac.id, [3]arif.susilo@pelitabangsa.ac.id

Abstract

In a company there must be an information exchange interaction, both messages, data or images. For this exchange, an application that can send and receive information is needed, not infrequently a company uses social media as a means of exchanging information. In exchanging information related to company secrets, extra security is needed considering there are so many hacks on social media. Therefore, to work around this we need additional security that can hide the message without being noticed by others. From the hacking problem above the author tries to find additional security for the exchange of messages between company employees that is safe and unknown to others. .

Keywords*: Steganography, Secret Massage with Image, Image, LSB Steganography..*

Abastrak

Dalam sebuah perusahaan pasti terdapat sebuat interaksi pertukaran informasi baik pesan, data ataupun gambar untuk pertukaran tersebut di butuhkan sebuah aplikasi yang dapat mengirim dan menerima sebuah informasi, tak jarang sebuah perusahaan menggunakan social media sebagai alat pertukaran informasi. Dalam pertukaran informasi yang berkaitan dengan rahasia perusahaan di butuhkan keamanan yang sangat extra mengingat banyak sekali peretasan terhadap social media. Oleh karena itu untuk menyiasatinya kita membutuhkan kemanan tambahan yang dapat menyembunyikan pesan tersebut tanpa di ketahui oleh orang lain. dari permasalahan peretasan diatas penulis berusaha mencari keamanan tambahan untuk pertukaran pesan antara karyawan perusahaan yang aman dan tidak diketahui orang lain, kemudian penulis menemukan Steganografi yaitu teknik menyembunyikan pesan kedalam gambar jadi selain si pengirim dan si penerima tidak akan tahu bahwa gambar tersebut berisi pesan. Untuk metodenya penulis mengambil Leas Significant Bit karena dalam penerapannya wadah untuk mengisi pesan lebih banyak.

Kata kunci: Steganografi, Secret Massage with Image, Image, Steganografi LSB.

1. Pendahuluan

1.1. Latar Belakang

Teknologi informasi berkembang pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Dengan adanya kemajuan ini data atau informasi yang tersedia pun sudah berubah menjadi digital. Data atau informasi dalam bentuk ini belum tentu aman karena dengan berkembangnya teknologi maka orang yang tidak memiliki akses seperti hacker juga semakin berkembang sehingga dapat menyebabkan data atau informasi dimanipulasi seperti diubah, dihilangkan, ataupun diduplikat dan hal yang dapat kita lakukan untuk menyelesaikan permasalahan keamanan ini adalah dengan menerapkan Steganografi.

PT Bank Tabungan Negara merupakan salah satu perusahaan Perbankan Milik BUMN yang sudah tersebar di seluruh daerah Indonesia. Didalam ruang lingkup pekerjaan perlu adanya pertukaran informasi yang bersifat rahasia, maka dari itu untuk menjaga

informasi melalui Sosial Media perlu keamanan ganda.

Sistem yang sedang berjalan secara di PT Bank Tabungan Negara adalah menggunakan Sosial Media sebagai media untuk bertukar informasi. Keamanan Pertukaran informasi karyawan di PT Bank Tabungan Negara selama ini, masih melakukan pengamanan Secara standart dengan memanfaatkan aplikasi pihak ketiga seperti Sosial Media.

Pada kesempatan ini penulis melakukan Observasi terhadap tingkat peretasan yang terjadi sepanjang 2021 di Indonesia. Penulis mengaitkan masalah yang terjadi dengan Jurnal terdahulu yang berkaitan dengan keamanan tambahan dengan Teknik Steganografi dan akan meneliti terkait keamanan Pesan rahasia.

Dengan teknik Steganografi pesan asli yang ingin dikirimkan (plaintext) disisipkan kedalam gambar yang tidak dapat terbaca oleh kasat mata, dengan mengirimkan gambar yang berisi pesan rahasia maka Hacker ataupun penyadap tidak akan menetahui bahwa gambar tersebut memiliki pesan didalamnya yang hanya bisa di buka oleh Aplikasi Khusus (Ahmad, 2017)10.

Dengan begitu, orang lain tidak akan menyadari bahwa gambar tersebut memiliki pesan, walaupun Whatsapp atau Email diretas siperetas pun tidak akan menyadari bahwa gambar tersebut memiliki pesan tersembunyi dan hanya bisa di buka oleh Aplikasi Khusus. Dan karena sifatnya manipulatif tidak timbul suatu kecurigaan terhadap pesan yang dikirim. Karena, Pesan akan disembunyikan di dalam gambar dan akan terlihat seperti gambar biasa. Di dalam sistem Steganografi, karyawan dapat menyembunyikan pesan di dalam gambar dan dapat mengirimkan ke Penerima kemudian penerima akan membuka pesan tersebut di Aplikasi System Steganografi.

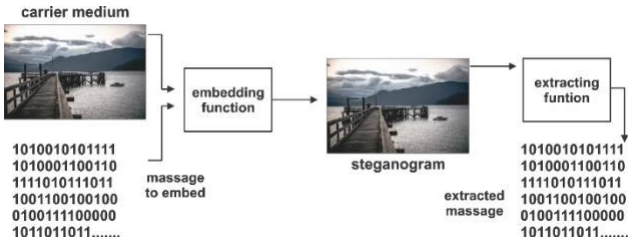
Pada pengimplementasian System Steganografi ini penulis menggunakan Metode Least Significant Bit dengan tujuan mampu memuat atau memasukan pesan lebih banyak pada gambar. Maka pada penelitian ini, penulis mencoba mengimplementasikan sistem untuk menjaga keamanan Informasi. Berdasarkan uraian diatas maka penulis mengangkat judul "Implementasi Steganografi dengan Metode Least Significant Bit (LSB) berbasis Web"..

2. Metode Penelitian

Metode Least Significant Bit

Pengubahan LSB (Least Siqnificant Bit) pada citra yang terkompresi sangat sulit diketahui secara kasat mata, sehingga metode ini sangat banyak digunakan. Metode ini memanfaatkan ketidak manpuan mata manusia dalam menemukan perbedaan antara gambar asli dengan yang sudah dimasukkan pesan. Pada Gambar 2.4 ditunjukan bahwa medium pembawa yang disisipkan pesan dengan menggunakan suatu fungsi penyisipan, dalam hal ini LSB , menghasilkan Stego-Image yang tidak mengalamai perubahan yang significant dari gambar aslinya (Muhammad Firdaus, 2019)[10].

2.1 least Significant Bit



Gambar 1 Least Significant Bit Sumber (Muhammad Firdaus, 2019)[10].

Untuk menjelaskan metode ini, digunakan citra digital sebagai Image Objek. Setiap Pixel dalam citra digital berukuran 1sampai 3 byte . pada susunan bit didalam byte (1 byte = 8 bit atau 8 binner), terdapat bit yang kurang berarti (Least Significant Bitatau LSB). Misalnya pada byte 00110011, maka bit LSB nya adalah bit yeng terletak paling kanan yaitu 1. Untuk melakukan penyisipan pesan, bit paling cocok untuk diganti denganbit pesan adalah bit LSB, sebab pengubahan bit tersebut hany akan mengubah nilai byte-nya menjadi satu lebih tinggi atau satu lebih rendah (Muhammad Firdaus, 2019)[10].

Sebagai contoh, urutan bit berikut ini menggambarkan 3 Pixel pada Cover-Image 24 bit.

(01010110 10111001 10000110)

(10001001 10001010 00010011)

(01011110 01111000 10101010)

Pesan yang akan disisipkan adalah karakter "M" , yang nilai binernya adalah 10010011, maka yang aka dihasilkan Stego-Image denganurutan bit sebagai berikut :

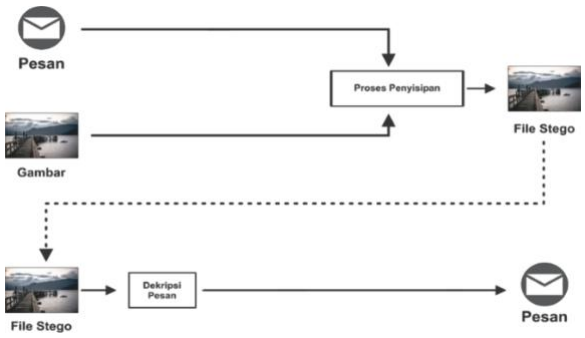
(01010111 10111000 10000110)

(10001001 10001010 00010010)

(01011111 01111001 10101010)

Perubahan yang tidak significant ini tidak akan tertangkap oleh indra manusia (jika media wadah adalah gambar, audio dan video). Dalam contoh diatas penggantian pixel tak significant dilakukan secara terurut. Penggantian pixel tak significant juga dapat dilakukan secara tidak terurut, bahkan hal ini dapat meningkatkan tingkat keamanan data(Muhammad Firdaus, 2019)[10].

2.2 Alur System



Gambar 2 Alur System **Sumber :** Penulis (2022)

Tahapan System dapat dilihat pada Gambar 3.2 Terlihat pada StegoBitmap mempunyai dua buah model utama yang memprementasikan dua buah fungsi utama yang sudah disebutkan pada subbab sebelumnya, yaitu model penyisipan pesan dan modul ekstraksi pesan

Pesan : Plaint Text atau isi text adalah tahapan untuk mengisi yang ingin disisipi

Gambar : gambar atau images berformat .jpg adalah tahapan untuk menginput gambar untuk wadah text

Proses Pentisipan : adalah Proses penyisipan

File Stego : adalah file output gambar yang telah disisipi pesan

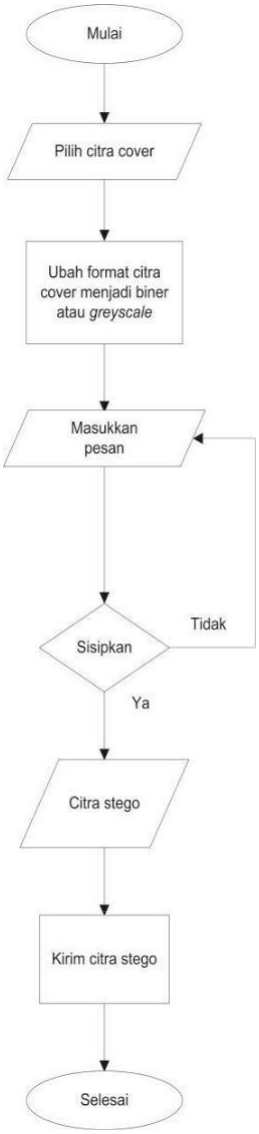
Dekripsi pesan : pemecahan File stego dengan Plain text

2.3 Flow Encode

Tahap Encode steganografi merupakan tahap dimana dilakukannya penyisipan karakter pesan kedalam citra cover. Langkah awal pada tahap ini adalah memilih citra yang akan digunakan sebagai citra cover. Citra yang dipilih akan merupakan citra RGB yang mana dalam citra tersebut akan diubah menjadi citra biner.

Citra cover yang sudah diubah menjadi biner berarti sudah siap untuk disisipkan oleh karakter pesan. Pesan yang disisipkan mempunyai limit atau batas yaitu sama dengan panjang dari ukuran citra cover. Karakter pesan yang akan disisipkan kedalam citra harus sudah dalam bentuk sekumpulan bit. Sekumpulan bit tersebut yang akan disisipkan kedalam citra, dimana letak dari sekumpulan bit tersebut akan ditempatkan pada akhir baris citra cover, hal tersebut menyebabkan ukuran citra cover bertambah.

Setelah penyisipan selesai dilakukan maka citra stego akan dikirimkan kepada penerima, yang mana pada sisi penerima akan dilakukan proses Decode steganografi, yang mana pada proses ini akan dilakukan pengungkapan pesan yang telah disisipkan sebelumnya..



Gambar 3 Flow Chart Encode **Sumber :** Penulis (2022)

2.4 Flow Decode

Proses yang kedua adalah proses Decode steganografi merupakan tahap diungkapkannya kembali pesan

yang telah disisipkan, sehingga penerima dapat memahami pesan yang terkandung didalam citra stego. Pada tahap desteganografi ini terdapat proses manipulasi citra yang mana citra stego akan diberikan noise (blurring dan salt and pepper), diubah letak pikselnya (rotation 900), dan diperbaiki kualitasnya (sharpen).

Tujuan dilakukkan tahap edit citra adalah untuk meneliti dan menganalisa ketahanan citra stego jika diberikan efekn tertentu, apakah pesan yang disisipkan tetap utuh atau akan rusak dan tidak dapat dipahami. Diagram alir proses desteganografi ditampilkan :

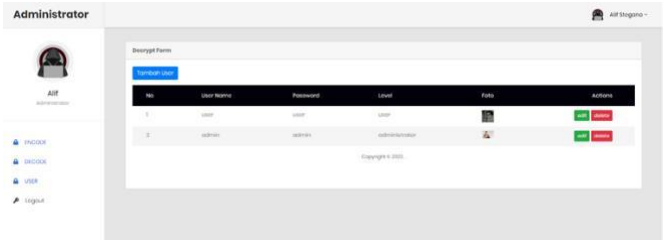
Gambar 4 Flow Chart Decode Sumber : Penulis (2022)

3. Hasil dan Pembahasan

Hasil dari penelitian yang didapatkan ada beberapa impelementasi sistem yang didapatkan, yaitu sebagai berikut :

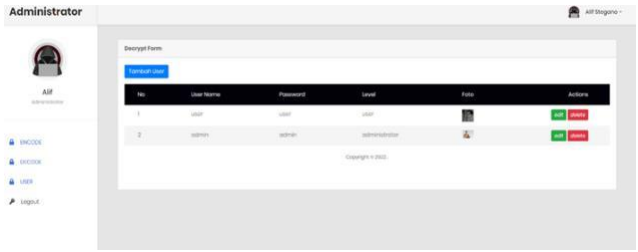
Gambar 5 Tampilan Login **Sumber :** Penulis (2022)

Dalam Tampilan login terdapat username dan password yang sudah terintegerasi dengan database dan dilengkapi dengan encrypt MD5.



Gambar 6 Halaman *Admin* **Sumber :** Penulis (2022)

Halaman *admin* adalah bagian menu yang hanya digunakan oleh *admin* (pemilik). Dimenu ini *admin* bisa melakukan perintah di aplikasi untuk menambah data, mengedit data dan menghapus data Pengguna.

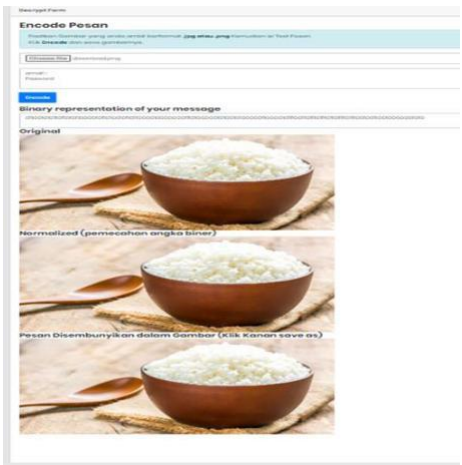


Gambar 7 Tambah User **Sumber :** Penulis (2022)

Halaman tambah *user* adalah tampilan dari aplikasi untuk menambahkan *user*, hal ini hanya dilakukan oleh *admin*.

Gambar 8 Enkode **Sumber :** Penulis (2022)

Setelah login berhasil maka akan masuk ke tampilan Encode, dalam menu ini berfungsi untuk encode gambar atau menyisipkan text kedalam gambar, ada tombol input gambar dan input text di dalamnya.

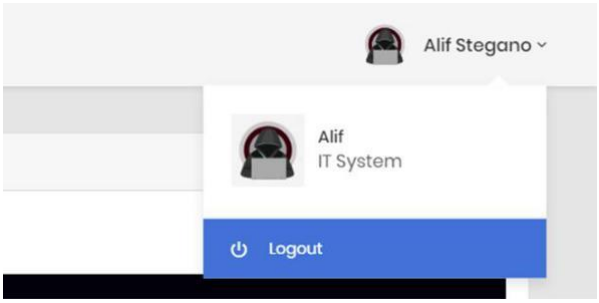


Gambar 9 Tampilan setelah Gambar di Enkode **Sumber** : Penulis (2022)

Setelah kita memasukan gambar dan text maka tampilanya akan berubah menjadi 3 gambar beserta keteranganya.

Gambar 10 Halaman *Decode* **Sumber :** Penulis (2022)

Dalam tampilan Decode atau mengungkapkan isi text dalam gambar terdapat tombol input gambar dan Decode.



Gambar 11 Halaman *Logout* **Sumber :** Penulis (2022)

Halaman logout adalah tampilan menu aplikasi bagi user dan admin yang ingin logout dari sistem aplikasi.

Peneliti juga melakukan pengujian terhadap sistem yang telah dibangun. Pengujian dilakukan dengan tujuan untuk mengamati hasil input dan output pada sistem. Pada pengujian ini dilakukan dengan pengujian Black-box, pengujian ini dapat menguji perangkat lunak tanpa harus mengetahui struktur kode dari perangkat lunak ini. Berikut hasil report dari pengujian black box yang telah dilakukan. Berikut hasil report dari pengujian black box yang telah dilakukan.

Pengujian Pertama dilakukan untuk menguji kebenaran validasi format gambar sebagai masukan pada proses penyisipan dan ekstraksi. Cara yang dilakukan adalah memasukkan format gambar jpg, dimana pengujian dinyatakan berhasil jika proses penyisipan dapat dilakukan pada gambar dengan format jpg.

Tabel 1 Hasil Pengujian Pertama

File Gambar	Format	Hasil Validasi	Kesimpulan
“Pemandangan1”	.jpg	Valid	Sukses
“Pemandangan2”	.jpg	Valid	Sukses
“Pemandangan3”	.jpg	Valid	Sukses
“Pemandangan4”	.jpg	Valid	Sukses

Dari hasil tersebut, terbukti bahwa StegoBitmap telah berhasil menjalankan fungsi parsing gambar BMP, sehingga validasi format gambar atau pengambilan nilai dalam gambar dapat dilakukan dengan baik.

Pengujian ini dilakukan dengan cara meyisipkan text ke dalam gambar, kemudian mengekstraksinya kembali. File yang digunakan sebagai bahan percobaan adalah file yang berbeda. Gambar yang menjadi media pada pengujian ini adalah gambar yang dinyatakan valid dari hasil kasus uji Pertama.

Hasil penyisipan pesan ini ditunjukkan pada table 2. untuk hasil pengujian dari gambar asli dengan gambar yang telah disisipkan pesan dapat dilihat pada hasil pengujian uji kasus kedua.

Tabel 2 Hasil Pengujian Kasus Uji 2 (Penyisipan)

Gambar	Text	Output	keterangan
Pemandangan.jpeg	testing	Pemandangan.png	Diterima
Pemandangan.jpeg	Email Password	Pemandangan.png	Diterima
Pemandangan.jpeg	Kode : 211221	Pemandangan.png	Diterima

Pengujian Ketiga ini dilakukan untuk menguji kualitas dari gambar yang dihasilkan setelah melalui proses penyisipan, yaitu dengan membandingkannya dengan gambar yang asli. Dimana perbandingan dari dua gambar hanya dilakukan secara subjektif (gambar dianggap mirip).

Tabel 3 Hasil Pengujian Kasus Uji Ketiga

Text yang disisipkan	File Gambar asli	File gambar setelah disisipkan
test		
Email password		

Tetapi dalam hal ini penulis ingin memberikan perbedaan secara kontras bahwa file yang telah disisipi lebih terang disbanding file asli.

Pengujian ini dilakukan dengan megirim Image yang sudah disisipkan file melalui Sosial Media. Kemudian melakukan pengungkapan (ekstrak) kembali terhadap Image yang dikirim.

Tabel 4 Hasil Pengujian Kasus Uji Keempat

Text yang disisipkan	File Gambar asli	Pengungkapan
test		Berhasil
Email password		Berhasil

4. Kesimpulan

Dari kegiatan-kegiatan yang telah dilakukan terkait dengan pelaksanaan tugas akhir, dapat disimpulkan bahwa pengimplementasian sistem Steganografi dengan metode Least Significant Bit untuk memanipulasi pesan saat pertukaran informasi oleh pihak ke tiga telah berhasil di lakukan dan dengan metode tersebut kita juga dapat memperbesar wadah agar memuat lebih banyak text.

Ucapan Terima Kasih

Dengan memanjatkan puji syukur kepada Allah SWT, yang Maha Pengasih dan Penyayang yang telah melimpahkan segala Anugrah KasihNya kepada Penulis, sehingga laporan Skripsi dengan Judul ”Implementasi Steganografi menggunakan metode Least Significant Bit berbasis WEB” dapat diselesaikan sesuai dengan rencana karena dukungan dari berbagai pihak yang tidak ternilai besarnya..

Referensi

[1] Davis, William S, Sistem Analisys and Design : A Structured Approach, United State of America: Addison-Westley Publishing Company.

[2] Ferry Pangaribuan, Aplikasi Penyembunyian Pesan Metode MARS Metode dan Zhang LSB Image. Bandung : Institut Teknologi Bandung, 2018.

[3] Gonzales, R.C., Woods, R.E. Digital Image Processing, Addison-Wesley Publishing Company, 1992.

[4] Hernawan Sulistyanto., Kompresi Data Lossless dengan Metode Lempel-Zip, Teknik Elektro Universitas Muhammadiyah Surakarta, 2019.

[5] Muhammad Hakim, Implementasi Penyembuyian pesan dengan metode LSB, Bandung : Institud Teknologi Bandung, 2022.

[6] Muhamad Firdaus, penentuan kombinasi teknik kompresi untuk mendukung penyimpanan data akademik pada smartcard, Institud Teknologi Sepuluh Nopember.2019.

[7] Morkel, T., Eloff, J.H.P., Olivier, M.S. An Overview of Citra Steganography, 2018.

[8] Prasetyo Andy Wicaksono, Penyembunyian Pesan pada Citra GIF Menggunakan Metode Adaptif, Bandung : Institut Teknologi Bandung, 2019.

[9] Rinaldi Munir, Pengolahan Citra Digital dengan Pendekatan Algoritmik, Bandung : Informatika, 2019.

[10] Ronald Augustinus Penalosa, Steganografi Pada Citra dengan Format GIF Menggunakan Algoritma GifShuffle, Bandung: ITB, 2018.

[11] Suarga, M. Sc., M. Math., Ph. D., Algoritma Pemograman, Makassar 2004. TIK, Mengenal program Grafis, Yokyakarta :SMA Negeri 1 Yokyakarta. 2018.

[12] Winda Winanti, Penyembuyian pesan pada citra terkompresi JPEG menggunakan metode Spread Spectrum, Bandung : Institut Teknologi Bandung, 2022.

[13] Willy Sudiarto Raharjo, Aditya Wikan Mahastama Permodelan System Perangkat Lunak, Uses Case UML, Univ Kristen Duta Wacana, PSPL.

[14] N. Anas, U. Islam, and N. Sumatera, “Komunikasi antara Kognitif dan Kemampuan Berbahasa,” *Eunoia*, pp. 1–8, 2021, [Online]. Available: http://jurnaltarbiyah.uinsu.ac.id/index.php/eunoia/article/view/997/775.

[15] W. Wahyudi, D. Hartama, I. O. Kirana, S. Sumarno, and I. Gunawan, “Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun,” *J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 57–66, 2022, doi: 10.54082/jiki.19.

[16] M. Masnur, S. Alam, and M. Fikri Nasir, “Rancang

Bangun Sistem Keamanan Motor Dengan Pengenalan Sidik Jari Berbasis Arduino Uno," *J. Sintaks Log.*, vol. 1, no. 1, pp. 2775–412, 2021, [Online]. Available: https://jurnal.umpar.ac.id/index.php/sylog.

[17] J. Karman and A. Nurhasan, "Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, 2019, doi: 10.32767/jti.v11i1.451.

[18] T.-H. Lu, D.-R. Chen, and T.-L. Chiang, "呂宗學 1,* 陳端容 2 江東亮 3," *Taiwan J. Public Heal.*, vol. 34, no. 2, pp. 115–119, 2015.

[19] R.Maulana and R.M. Simanjorang, "Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, pp. 377–383, 2021, doi: 10.32672/jnkti.v4i6.3533.

[20] F. Fahrianto and A. Kitanggi, "Penerapan End-To-End Encryption Dengan Metode Super Encryption Untuk Kerahasiaan Citra Digital Pada Aplikasi Instant Messaging," *J. Tek. Inform.*, vol. 9, no. 1, pp. 1–8, 2016, doi: 10.15408/jti.v9i1.5651.

[21] A. Amiruddin and M. F. Rohmani, "Perancangan Spesifikasi Keamanan untuk Pengembangan Aplikasi Secure Chat Berdasarkan Common Criteria For It Security Evaluation," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 6, p. 1215, 2021, doi: 10.25126/jtiik.2021863637.

[22] H. Hasrul and L. H. Siregar, "Penerapan Teknik KriptografipadaDatabasemenggunakan Algoritma One Time Pad," *Elektron. Sist. Inf. dan Komput.*, vol. 2, no. 2, pp. 41–52, 2016, [Online]. Available: stmik-binamulia.ac.id.

[23] B. Fachri and R. M. Sembiring, "Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android," *J. Media Inform. Budidarma*, vol. 4, no. 1, p. 110, 2022, doi: 10.30865/mib.v4i1.1700.

[24] E. F. Ginting, K. Ibnutama, and M. G. Suryanata, "Implementasi DES (Data Encryption Standard) Untuk Penyandian Data Bill Of Material pada Divisi Produksi PT.Siantar Top, Tbk," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, p. 161, 2019, doi: 10.53513/jis.v18i2.155.